

# Exemple de configuration d'un VPN SSL sans client (WebVPN) sur Cisco IOS avec SDM

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Diagramme du réseau](#)

[Conventions](#)

[Tâches de préconfiguration](#)

[Configurer le WebVPN sur Cisco IOS](#)

[Étape 1. Configurez le webvpn gateway](#)

[Étape 2. Configurez les ressources permises pour le policy group](#)

[Étape 3. Configurez le policy group de webvpn et sélectionnez les ressources](#)

[Étape 4. Configurez le contexte de webvpn](#)

[Étape 5. Configurez la base de données utilisateur et la méthode d'authentification](#)

[Résultats](#)

[Vérifiez](#)

[Procédure](#)

[Commandes](#)

[Dépannez](#)

[Procédure](#)

[Commandes](#)

[Informations connexes](#)

## [Introduction](#)

Le VPN SSL sans client (WebVPN) permet à un utilisateur d'accéder en mode sécurisé à des ressources sur le LAN de l'entreprise depuis n'importe où avec un navigateur Web compatible SSL. L'utilisateur s'authentifie d'abord avec une passerelle WebVPN qui permet alors l'accès utilisateur à des ressources réseau pré-configurées. Des webvpn gateway peuvent être configurés sur des Routeurs de Cisco IOS®, des appliances de sécurité adaptable Cisco (ASA), des concentrateurs de Cisco VPN 3000, et le Module de services de webvpn de Cisco pour le Catalyst 6500 et 7600 Routeurs.

La technologie de réseau privé virtuel (VPN) Secure Socket Layer (SSL) peut être configurée sur des périphériques Cisco dans trois modes principaux : VPN SSL sans client (WebVPN), VPN SSL client léger (réacheminement de port) et client VPN SSL (SVC). Ce document explique la configuration de WebVPN sur des routeurs Cisco IOS.

**Remarque:** Ne changez pas le nom du domaine IP ni le nom d'hôte du routeur car cela déclenchera une régénération du certificat auto-signé et remplacera le point de confiance configuré. La régénération du certificat auto-signé entraîne des problèmes de connexions si le routeur a été configuré pour le WebVPN. WebVPN relie le nom du point de confiance SSL à la configuration de la passerelle WebVPN. Par conséquent, si un nouveau certificat auto-signé est émis, le nouveau nom du point de confiance ne correspond pas à la configuration WebVPN et les utilisateurs ne peuvent pas se connecter.

**Remarque:** Si vous exécutez la commande `ip https-secure server` sur un routeur WebVPN qui utilise un certificat auto-signé persistant, une nouvelle clé RSA est générée et le certificat devient incorrect. Un nouveau point de confiance est créé, ce qui casse le WebVPN SSL. Si le routeur qui utilise le certificat auto-signé persistant redémarre après que vous avez exécuté la commande `ip https-secure server`, le même problème se produit.

Référez-vous à [Exemple de configuration du VPN SSL \(WebVPN\) client léger sur IOS avec SDM](#) afin d'en savoir plus sur le VPN SSL client léger.

Référez-vous à [Exemple de configuration du client VPN SSL \(SVC\) sur IOS avec SDM](#) afin d'en savoir plus sur le client VPN SSL.

Le VPN SSL s'exécute sur les plates-formes de routeur Cisco suivantes :

- Routeurs de la gamme Cisco 870, 1811, 1841, 2801, 2811, 2821 et 2851
- Routeurs de la gamme Cisco 3725, 3745, 3825, 3845, 7200 et 7301

## [Conditions préalables](#)

### [Conditions requises](#)

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

- Image avancée du Logiciel Cisco IOS Version 12.4(6)T ou ultérieure
- Une des plates-formes de routeur Cisco mentionnées dans l'[Introduction](#)

### [Composants utilisés](#)

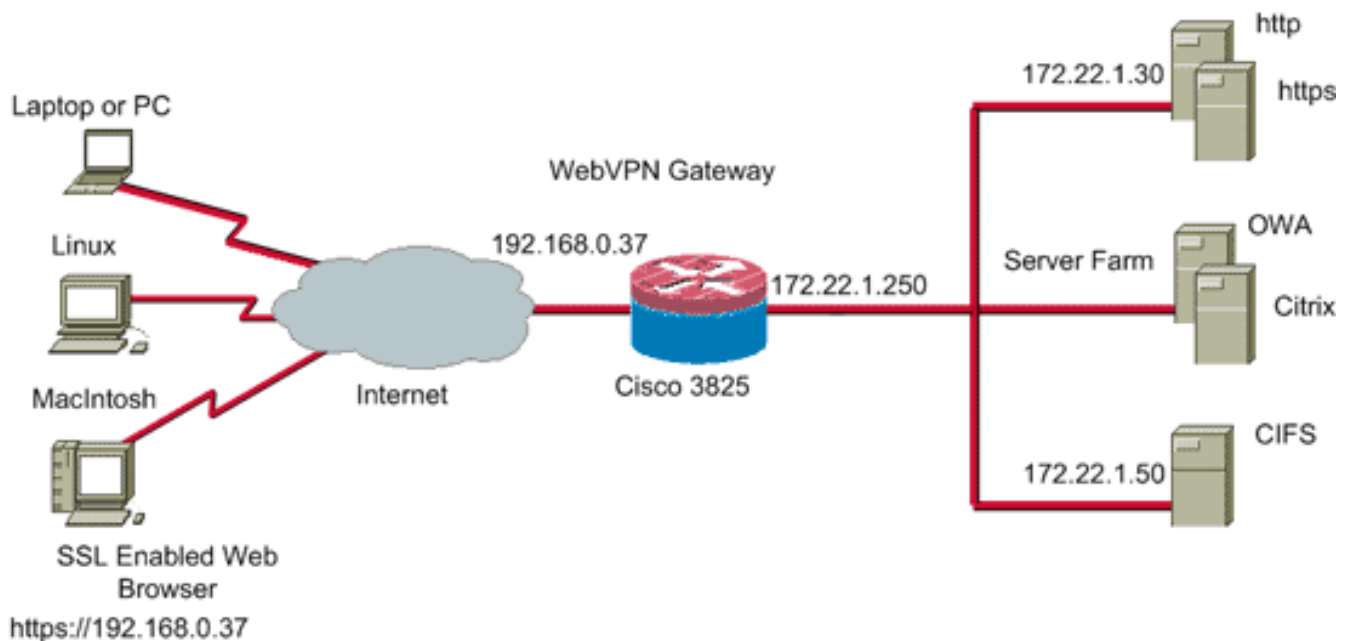
Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Routeur Cisco 3825
- Image logicielle Advanced Enterprise - Logiciel Cisco IOS Version 12.4(9)T
- Cisco Router and Security Device Manager (SDM) - version 2.3.1

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande. Les adresses IP utilisées dans cet exemple sont extraites des adresses RFC 1918 qui sont privées et ne sont pas utilisables légalement sur Internet.

### [Diagramme du réseau](#)

Ce document utilise la configuration réseau suivante :



## Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

## Tâches de préconfiguration

Avant de commencer, complétez ces tâches :

1. Configurez un nom d'hôte et un nom de domaine.
2. Configurez le routeur pour SDM. Cisco livre certains routeurs avec une copie préinstallée de SDM. Si Cisco SDM n'est pas déjà chargé sur votre routeur, vous pouvez obtenir une copie gratuite du logiciel à partir du site [Téléchargement de logiciel](#) ( [clients enregistrés](#) seulement). Vous devez avoir un compte CCO avec un contrat de service. Pour obtenir des informations détaillées sur l'installation et la configuration de SDM, référez-vous à [Cisco Router and Security Device Manager](#).
3. Configurez la date, l'heure et le fuseau horaire appropriés pour votre routeur.

## Configurer le WebVPN sur Cisco IOS

Vous pouvez avoir plus d'une passerelle WebVPN associée à un périphérique. Chaque passerelle WebVPN est liée à une seule adresse IP sur le routeur. Vous pouvez créer plus d'un contexte WebVPN pour une passerelle WebVPN donnée. Pour identifier les contextes individuels, donnez à chaque contexte un nom unique. Un groupe de stratégies peut être associé à un seul contexte WebVPN. Le groupe de stratégies décrit quelles ressources sont disponibles dans un contexte WebVPN particulier.

Complétez ces étapes afin de configurer le WebVPN sur Cisco IOS :

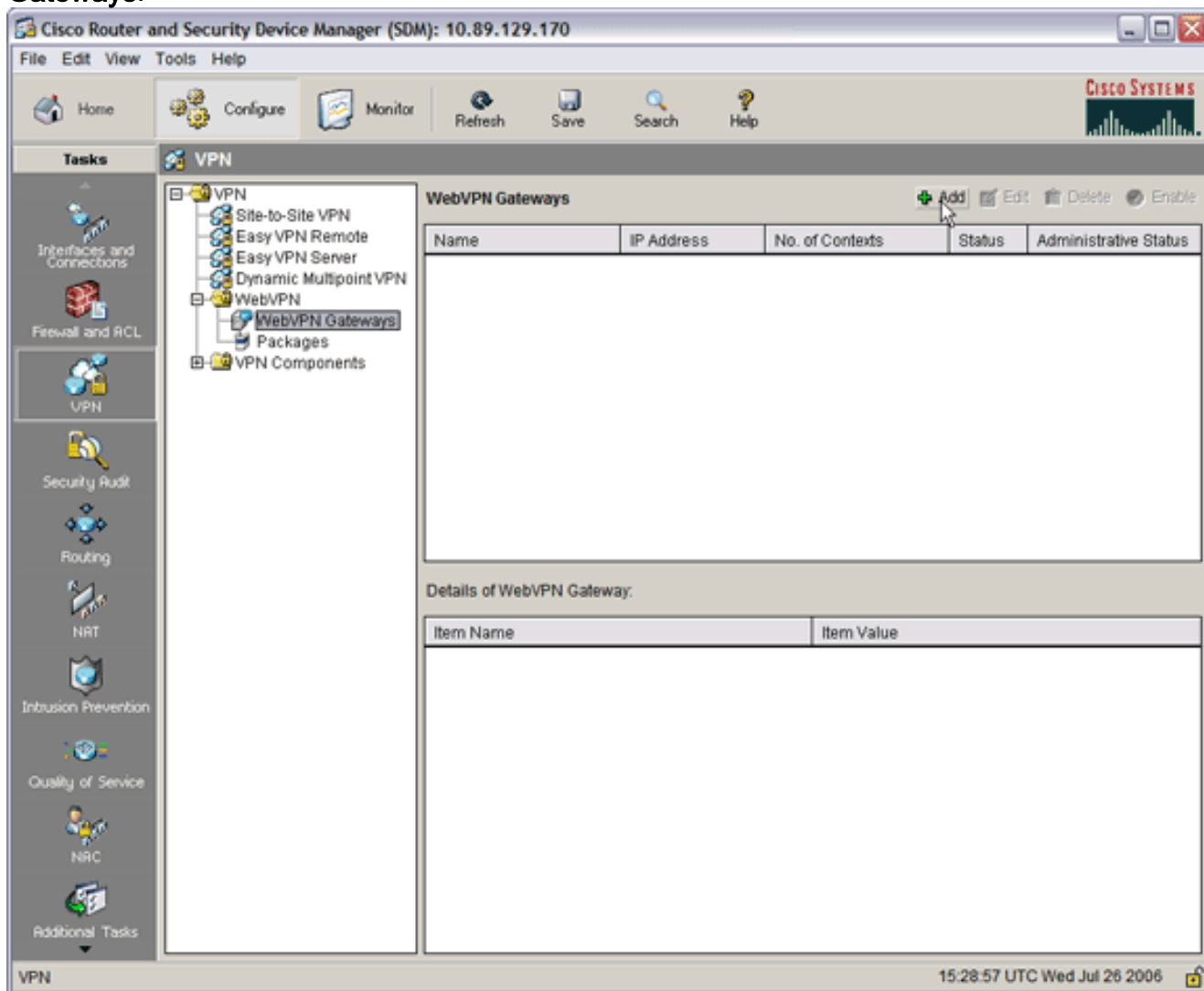
1. [Configurez la passerelle WebVPN](#)

2. [Configurez les ressources autorisées pour le groupe de stratégies](#)
3. [Configurez le groupe de stratégies WebVPN et sélectionnez les ressources](#)
4. [Configurez le contexte WebVPN](#)
5. [Configurez la base de données utilisateur et la méthode d'authentification](#)

## Étape 1. Configurez le webvpn gateway

Complétez ces étapes afin de configurer la passerelle WebVPN :

1. Dans l'application SDM, cliquez sur **Configure**, puis sur **VPN**.
2. Développez **WebVPN**, et choisissez **WebVPN Gateways**.



3. Cliquez sur **Add**. La boîte de dialogue Add WebVPN Gateway

**Add WebVPN Gateway**

Gateway Name:

Enable Gateway

IP Address

WebVPN clients will use this IP address and port number to connect to the WebVPN gateway.

IP Address:  ▼ Port:

Hostname:  (Optional)

Enable secure SDM access through 192.168.0.37

Digital Certificate

Digital Certificate configured under this trustpoint will be sent to the client for SSL authentication.

Trustpoint:  ▼

Redirect HTTP Traffic (Optional)

Configure HTTP redirect so that clients accessing the portal page using HTTP will be automatically redirected to the secure HTTPS service that WebVPN uses.

HTTP Port:

OK Cancel Help

apparaît.

4. Entrez des valeurs dans les zones Gateway Name et IP Address, et activez la case à cocher **Enable Gateway**.
5. Activez la case à cocher **Redirect HTTP Traffic**, puis cliquez sur **OK**.
6. Cliquez sur **Save**, puis sur **Yes** pour accepter les modifications.

## [Étape 2. Configurez les ressources permises pour le policy group](#)

Afin de faciliter l'ajout de ressources à un groupe de stratégies, vous pouvez configurer les ressources avant de créer le groupe de stratégies.

Complétez ces étapes afin de configurer les ressources autorisées pour le groupe de stratégies :

1. Cliquez sur **Configure**, puis sur **VPN**.

Cisco Router and Security Device Manager (SDM): 10.89.129.170

File Edit View Tools Help

Home Configure Monitor Refresh Save Search Help

Tasks

VPN

Site-to-Site VPN  
Easy VPN Remote  
Easy VPN Server  
Dynamic Multipoint VPN  
WebVPN  
WebVPN Gateways  
Packages  
VPN Components

Create WebVPN Edit WebVPN

SDM can guide you through WebVPN configuration tasks. Select a task, then click 'Launch the selected task' button.

Use Case Scenario

Recommended Tasks

DNS is not enabled on your router. As some WebVPN services require DNS to work, it is recommended that you enable DNS. [Enable DNS](#)

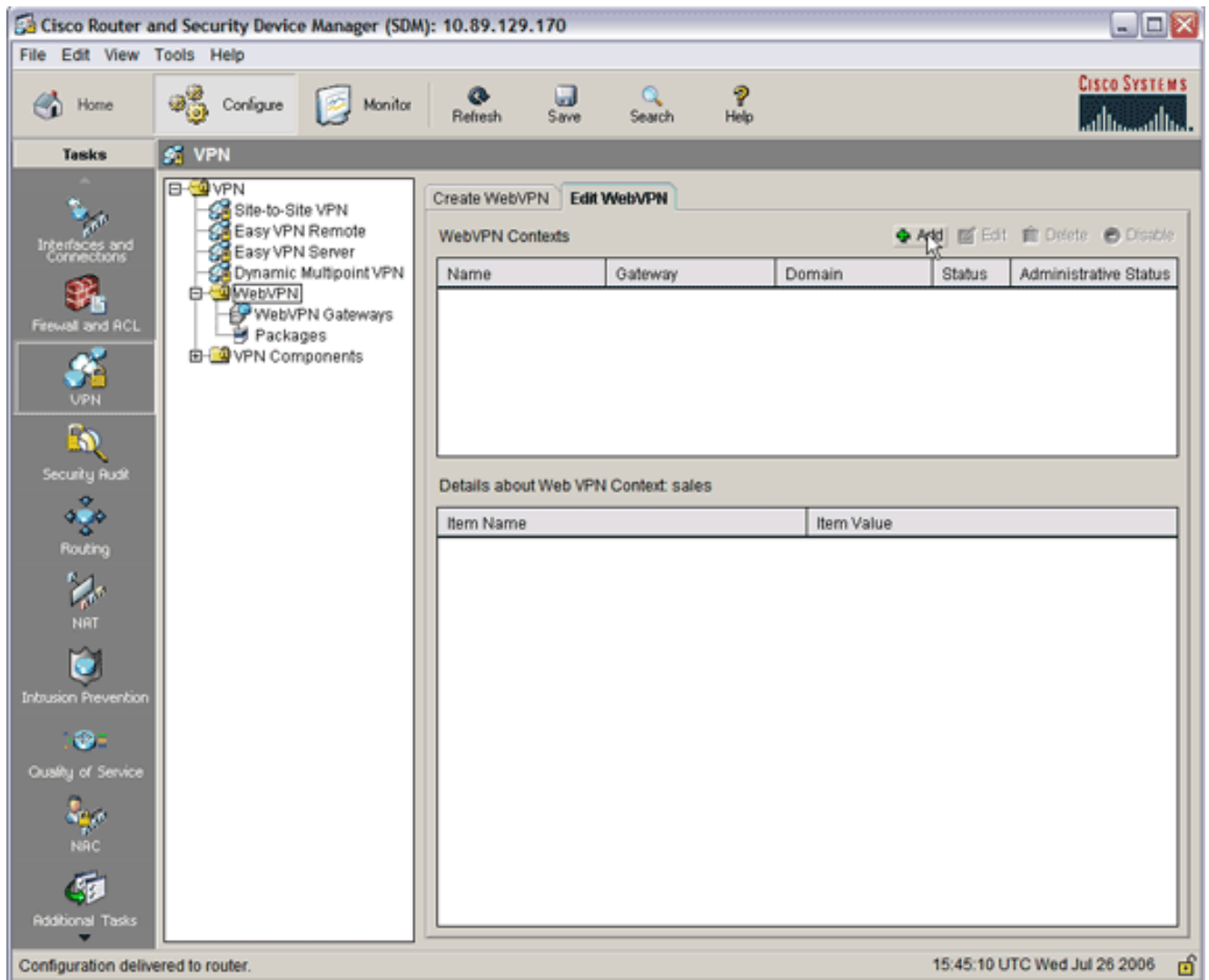
- Create a new WebVPN  
Use this wizard to create a new WebVPN.
- Add a new policy to an existing WebVPN for a new group of users  
Use this wizard to create a new policy to an existing WebVPN for a new group of users. For example you can create separate policies for different departments in your company.
- Configure advanced features for an existing WebVPN  
Use this wizard to configure advanced features such as thin client, full tunnel, and Cisco Secure Desktop for an existing WebVPN.

Launch the selected task

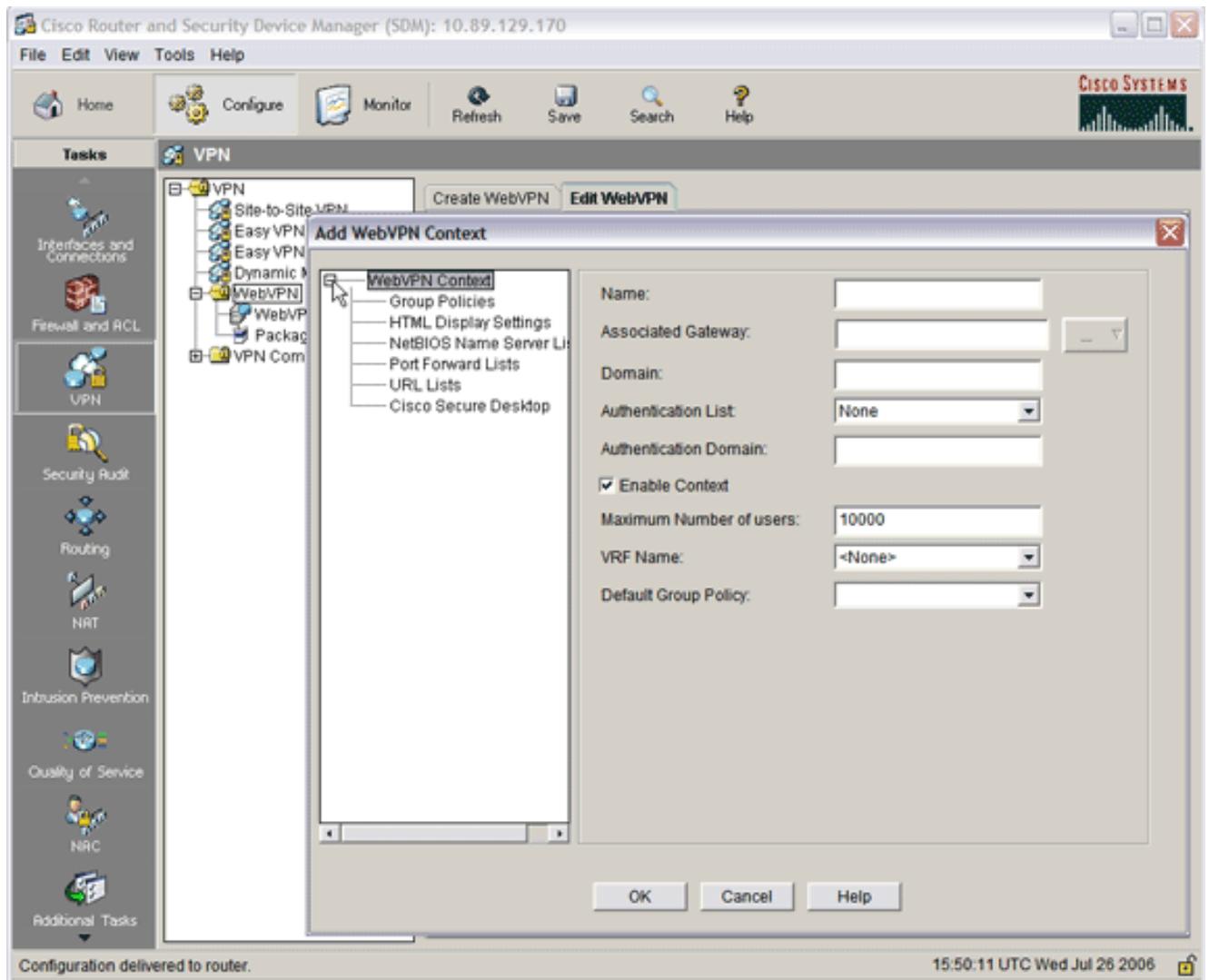
How do I:  Go

Running config copied successfully to Startup Config of your router. 15:40:55 UTC Wed Jul 26 2006

2. Choisissez **WebVPN**, puis cliquez sur l'onglet **Edit WebVPN** .**Remarque:** Le WebVPN vous permet de configurer l'accès pour la navigation HTTP, HTTPS et l'exploration de fichiers dans Windows à l'aide du protocole CIFS (Common Internet File System) et de Citrix.

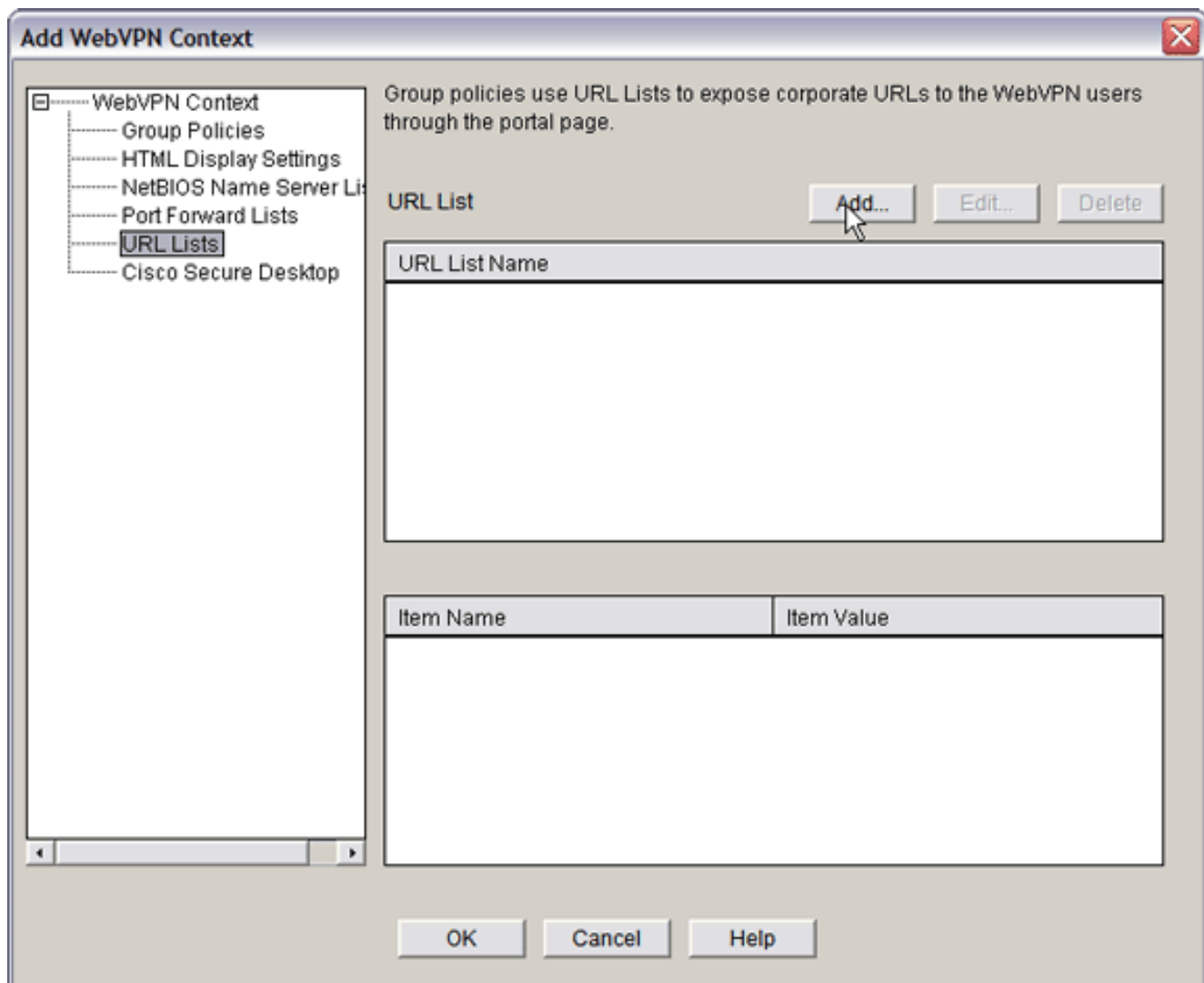


3. Cliquez sur **Add**. La boîte de dialogue Add WebVPN Context apparaît.

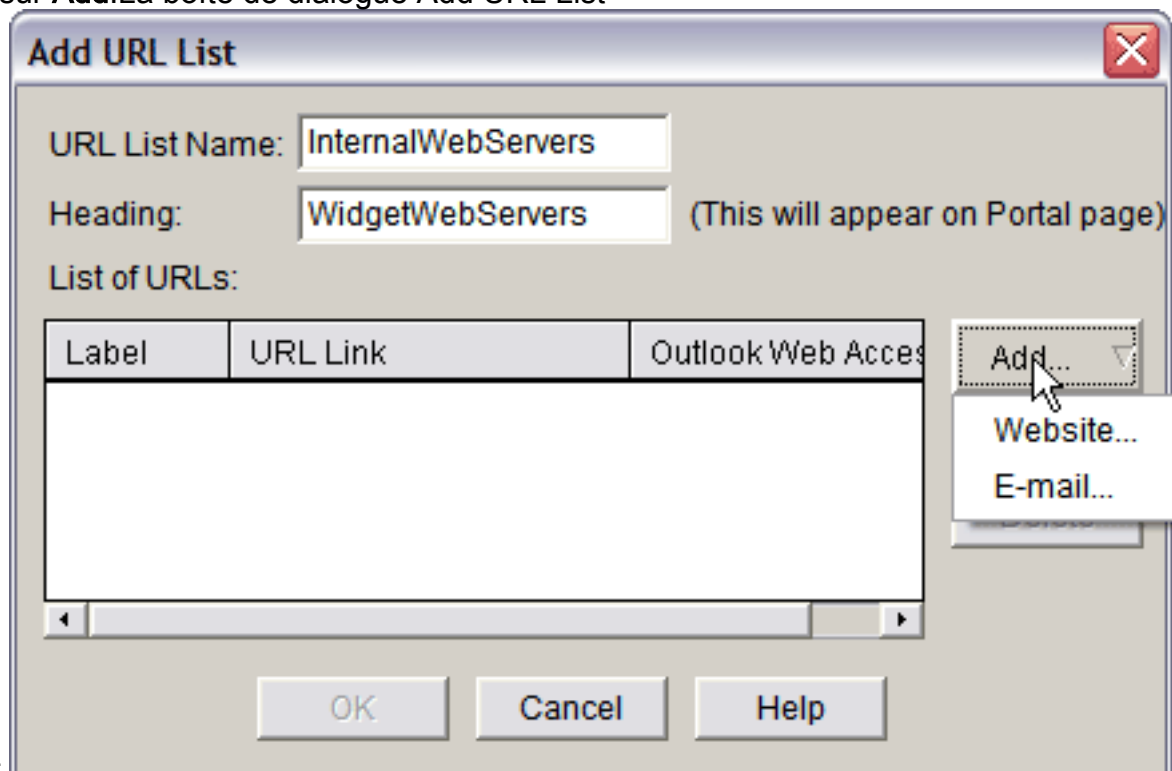


4. Développez **WebVPN Context**, et choisissez **URL Lists**.





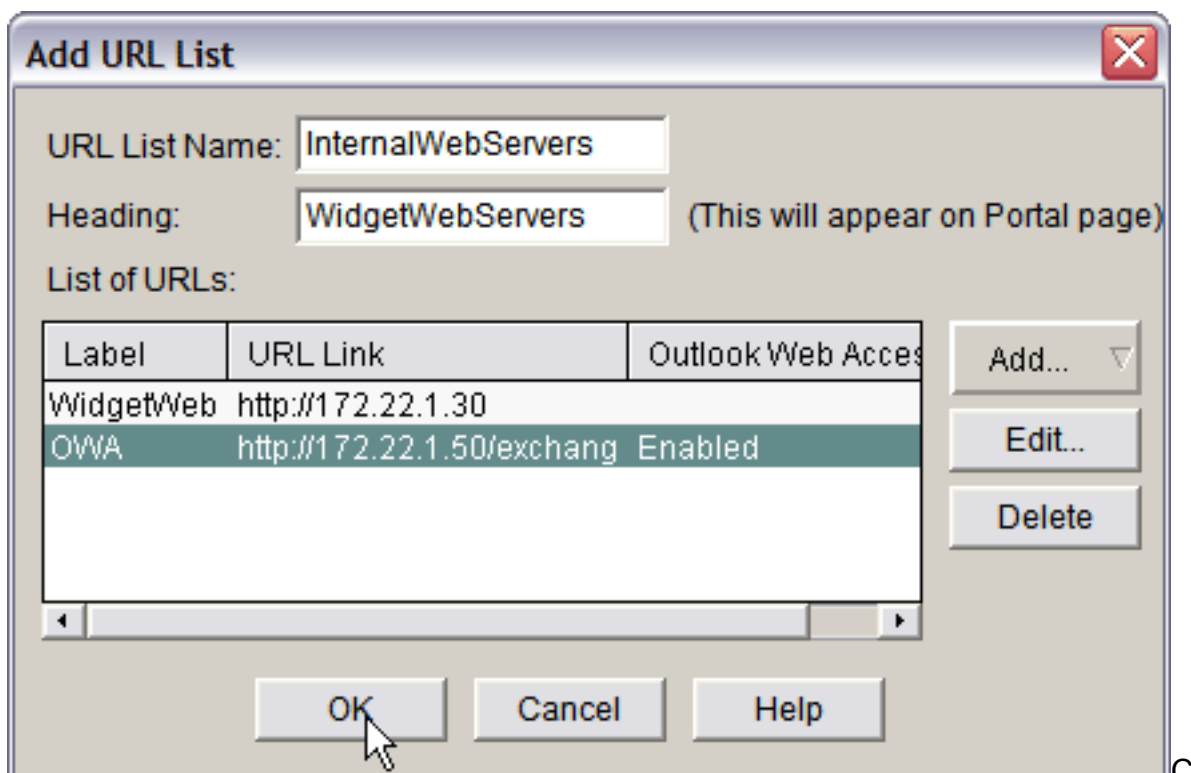
5. Cliquez sur **Add**. La boîte de dialogue Add URL List



apparaît.

6. Entrez des valeurs dans les zones URL List Name et Heading.

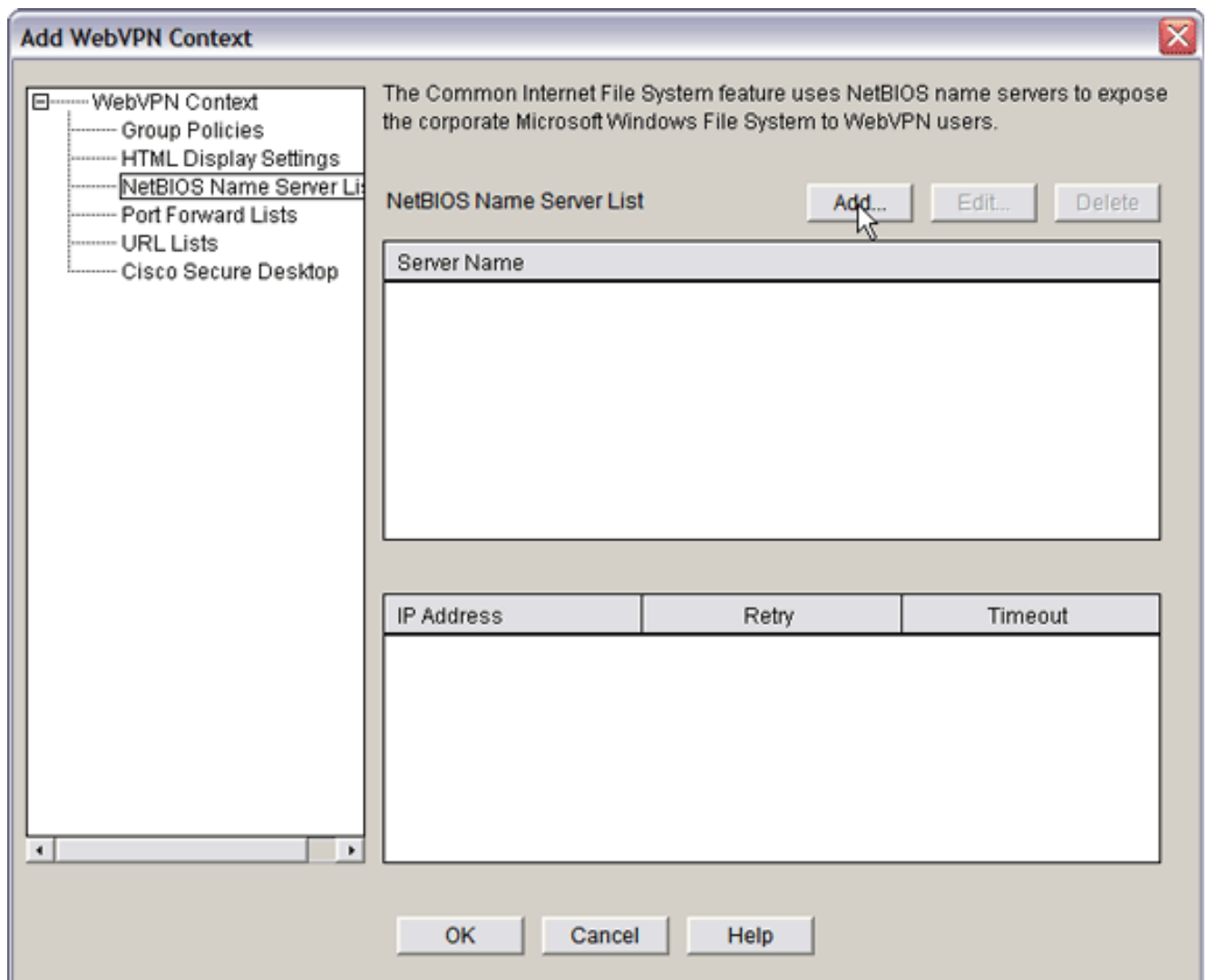
7. Cliquez sur **Add**, et choisissez



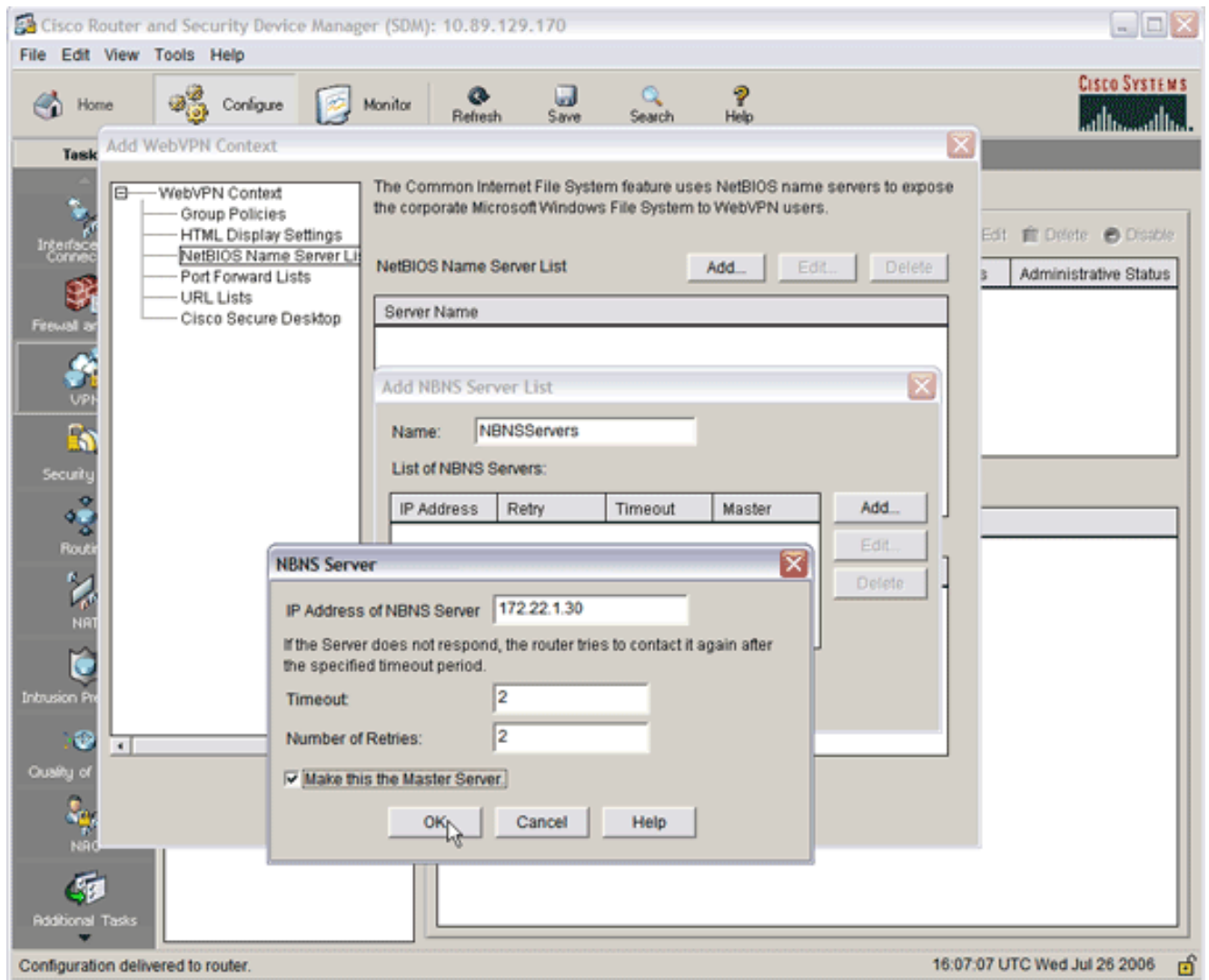
Website.

ette liste contient tous les serveurs Web HTTP et HTTPS que vous souhaitez voir disponibles pour cette connexion WebVPN.

8. Afin d'ajouter l'accès pour Outlook Web Access (OWA), cliquez sur **Add**, choisissez **E-mail**, puis cliquez sur **OK** après avoir rempli toutes les zones désirées.
9. Afin d'autoriser l'exploration de fichiers dans Windows via CIFS, vous pouvez indiquer un serveur NetBIOS Name Service (NBNS) et configurer les partages appropriés dans le domaine Windows. Dans la liste WebVPN Context, choisissez **NetBIOS Name Server Lists**.



Cliquez sur **Add**. La boîte de dialogue Add NBNS Server List apparaît. Entrez un nom pour la liste, et cliquez sur **Add**. La boîte de dialogue NBNS Server apparaît.

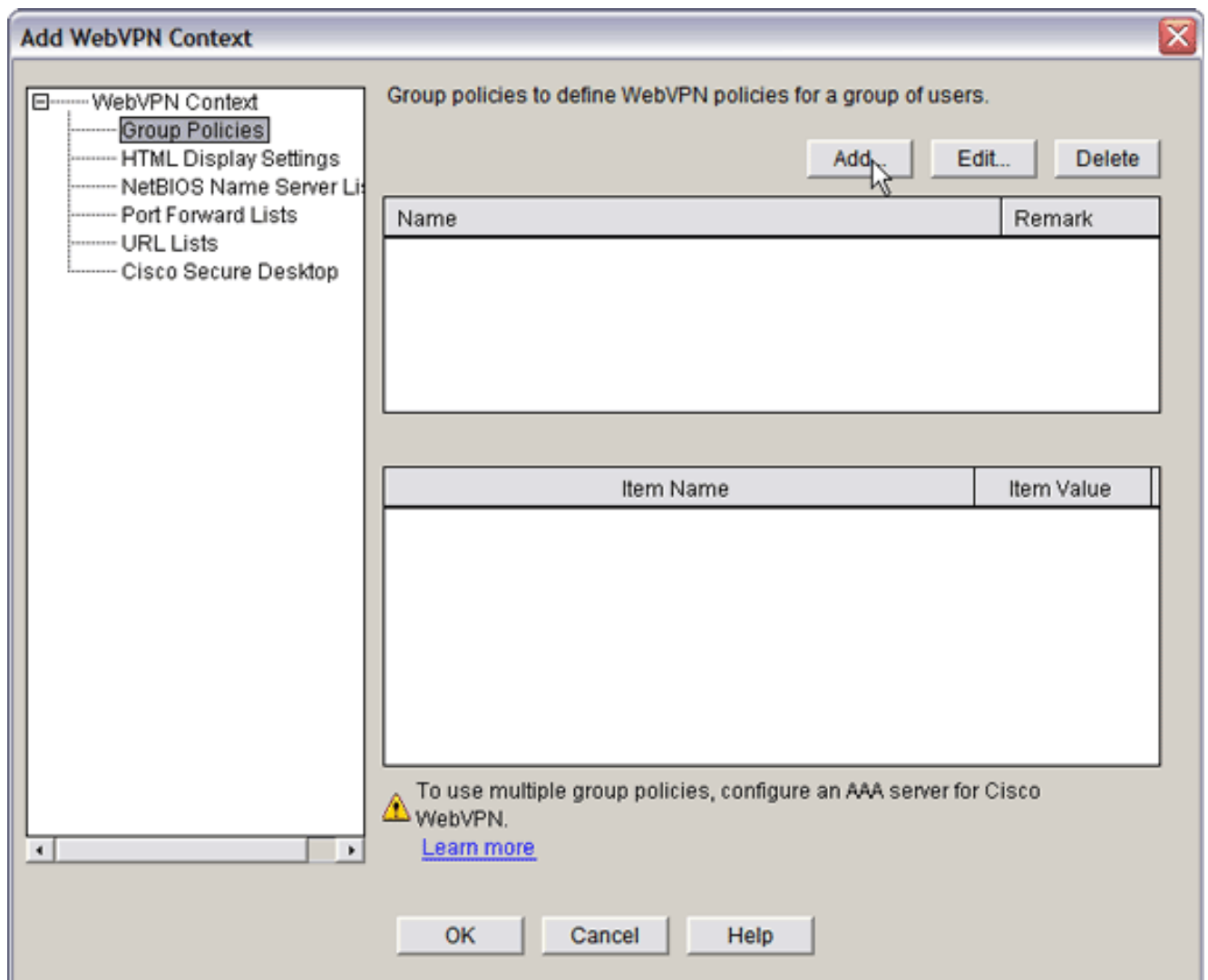


Le cas échéant, activez la case à cocher **Make This the Master Server** .Cliquez sur **OK**, puis sur **OK**.

### [Étape 3. Configurez le policy group de webvpn et sélectionnez les ressources](#)

Complétez ces étapes afin de configurer le groupe de stratégies WebVPN et de sélectionner les ressources :

1. Cliquez sur **Configure**, puis sur **VPN**.
2. Développez **WebVPN**, et choisissez **WebVPN Context**.



3. Choisissez **Group Policies**, et cliquez sur **Add**. La boîte de dialogue Add Group Policy apparaît.

**Add Group Policy**

General Clientless Thin Client SSL VPN Client (Full Tunnel)

Name:

**Make this the default group policy for context.**

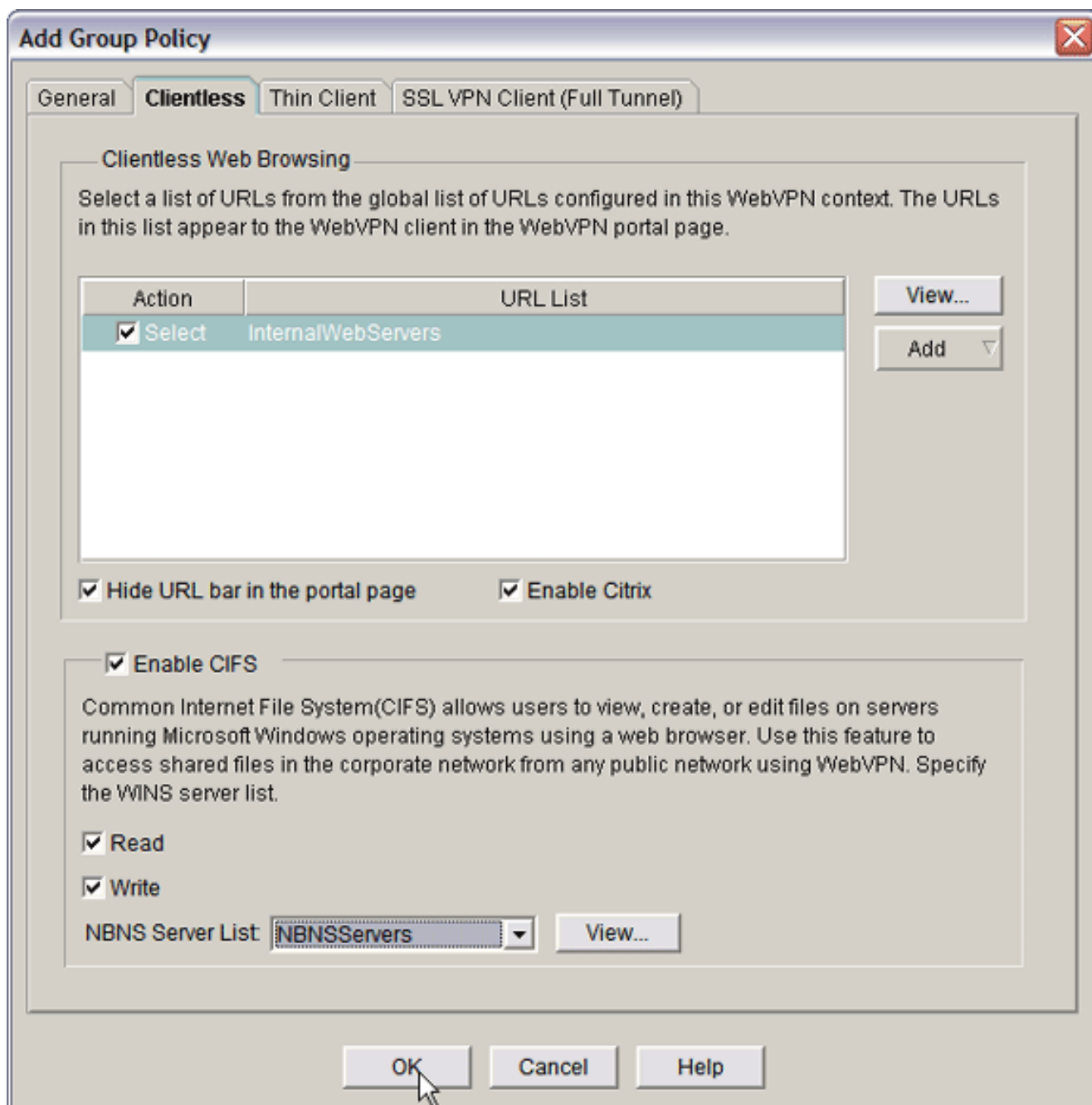
Timeouts

Client's WebVPN session will be disconnected if the client is connected longer than the session timeout or if the client is idle longer than the idle timeout.

Idle Timeout:  (sec)      Session Timeout:  (sec)

OK Cancel Help

4. Entrez un nom pour la nouvelle stratégie, et activez la case à cocher **Make this the default group policy for context.**
5. Cliquez sur l'onglet **Clientless** situé en haut de la boîte de dialogue.

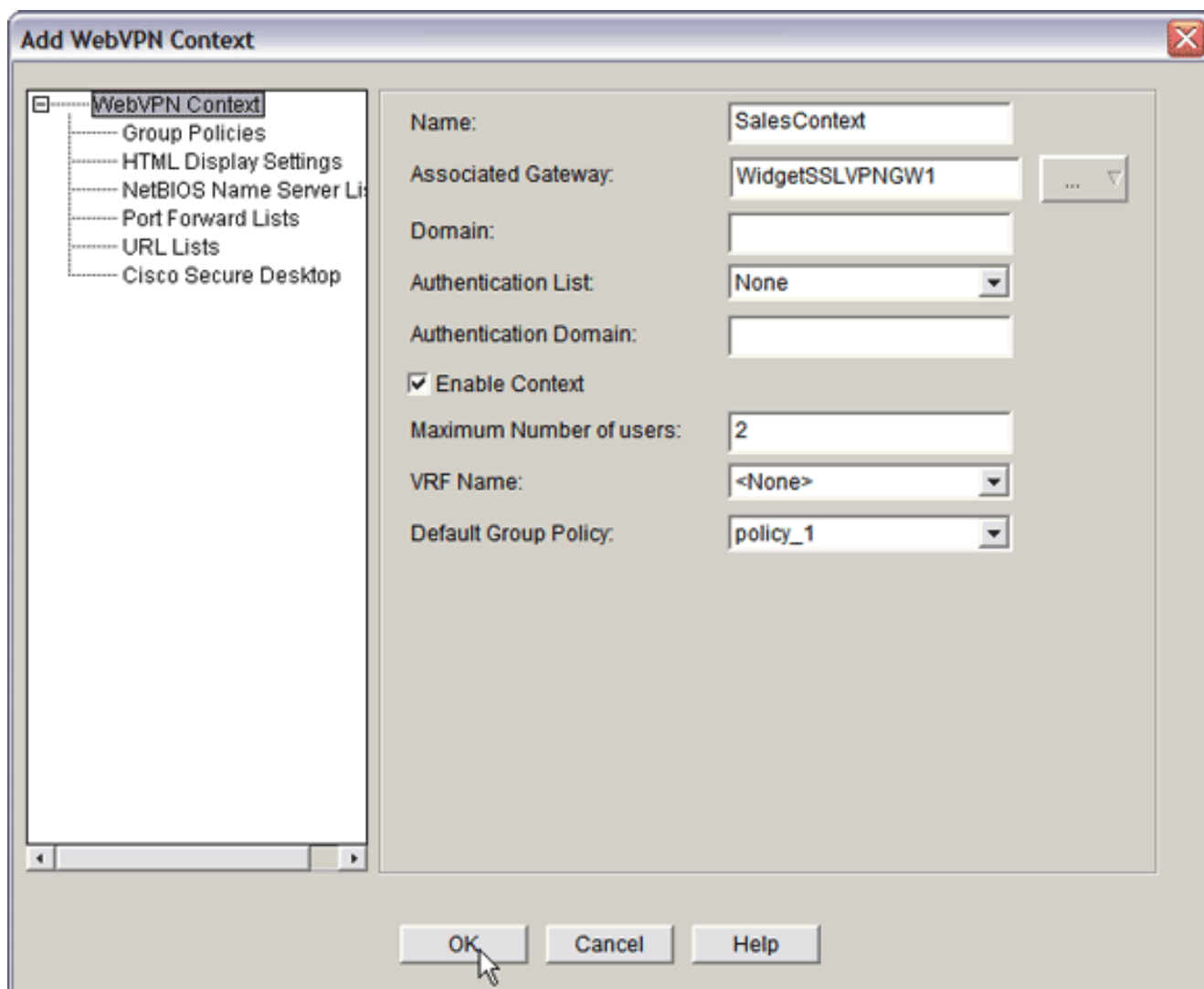


6. Activez la case à cocher **Select** pour la liste d'URL désirée.
7. Si vos clients utilisent les clients Citrix qui ont besoin de l'accès aux serveurs Citrix, activez la case à cocher **Enable Citrix** .
8. Activez les cases à cocher **Enable CIFS**, **Read** et **Write** .
9. Cliquez sur la flèche déroulante **NBNS Server List** et choisissez la liste de serveurs NBNS que vous avez créée pour l'exploration des fichiers dans Windows dans l'[Étape 2](#).
10. Cliquez sur **OK**.

#### [Étape 4. Configurez le contexte de webvpn](#)

Pour relier la passerelle WebVPN, la stratégie de groupe et les ressources ensemble, vous devez configurer le contexte webVPN. Complétez ces étapes afin de configurer le contexte WebVPN :

1. Choisissez **WebVPN Context**, et entrez un nom pour le contexte.



2. Cliquez sur la flèche déroulante Associated Gateway, et choisissez une passerelle associée.
3. Si vous avez l'intention de créer plus d'un contexte, entrez un nom unique dans la zone Domain pour identifier ce contexte. Si vous ne renseignez pas la zone Domain, les utilisateurs doivent accéder au WebVPN avec **https://IPAddress**. Si vous entrez un nom de domaine (par exemple, *Sales*), les utilisateurs doivent se connecter avec **https://IPAddress/Sales**.
4. Activez la case à cocher **Enable Context**.
5. Dans la zone Maximum Number of Users, entrez le nombre maximal d'utilisateurs autorisés par la licence du périphérique.
6. Cliquez sur la flèche déroulante **Default Group policy**, et sélectionnez le groupe de stratégies à associer avec ce contexte.
7. Cliquez sur **OK**, puis sur **OK**.

## [Étape 5. Configurez la base de données utilisateur et la méthode d'authentification](#)

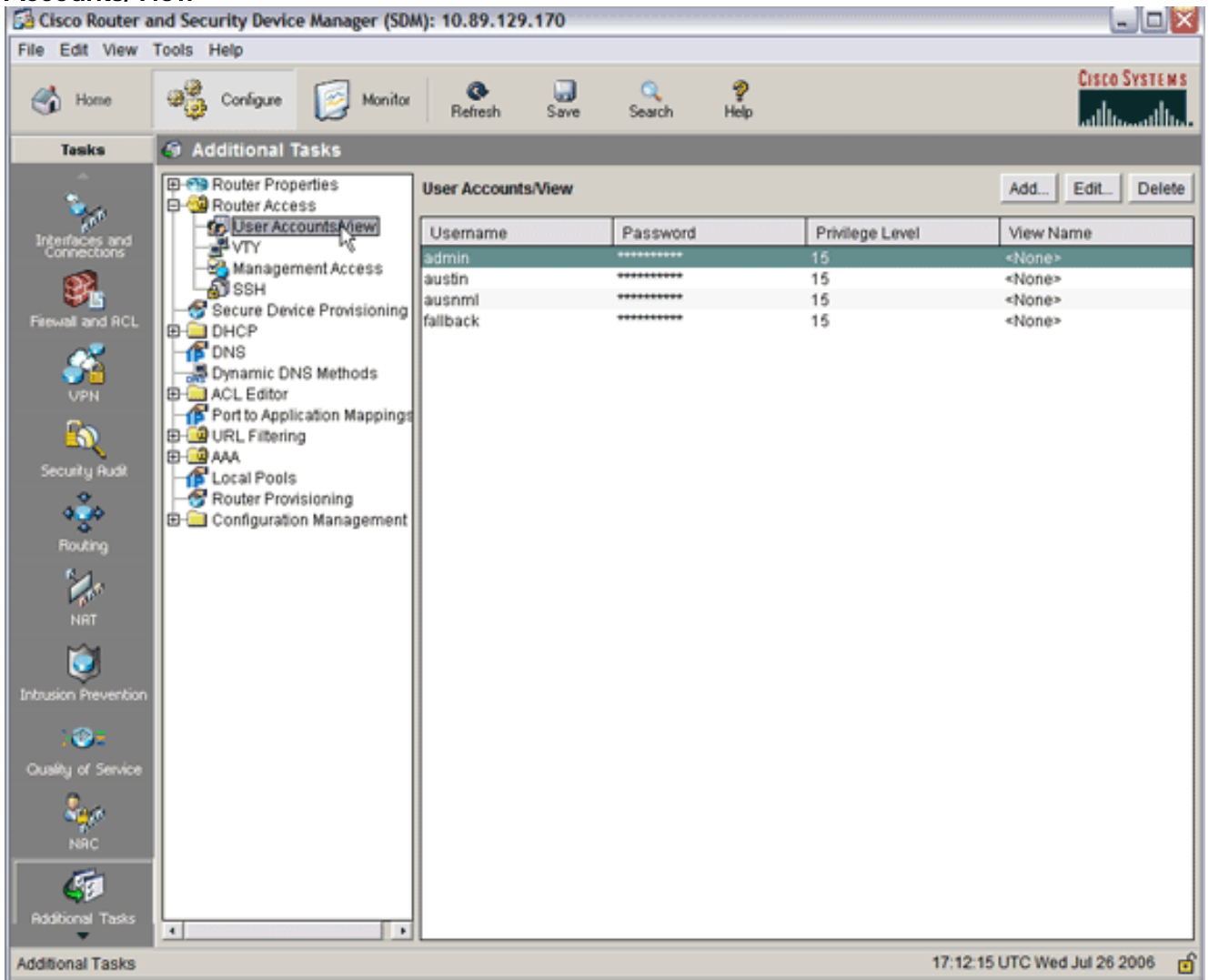
Vous pouvez configurer des sessions VPN SSL sans client (WebVPN) pour l'authentification auprès du serveur Radius, du Serveur Cisco AAA, ou d'une base de données locale. Cet exemple utilise une base de données locale.

Complétez ces étapes afin de configurer la base de données utilisateur et la méthode d'authentification :

1. Cliquez sur **Configuration**, puis sur **Additional Tasks**.



2. Développez **Router Access**, et choisissez **User Accounts/View**.



3. Cliquez sur le bouton **Add**. La boîte de dialogue Add an Account

**Add an Account**

Enter the username and password

Username:

Password:

New Password:

Confirm New Password:

Encrypt password using MD5 hash algorithm

Privilege Level:

Associate a View with the user

View Name:

apparaît.

4. Entrez un compte d'utilisateur et un mot de passe.
5. Cliquez sur **OK**, puis sur **OK**.
6. Cliquez sur **Save**, puis sur **Yes** pour accepter les modifications.

## Résultats

L'ASDM crée les configurations de ligne de commande suivantes :

```

ausnml-3825-01
Building configuration...

Current configuration : 4190 bytes
!
! Last configuration change at 17:22:23 UTC Wed Jul 26
2006 by ausnml
! NVRAM config last updated at 17:22:31 UTC Wed Jul 26
2006 by ausnml

```

```
!  
version 12.4  
service timestamps debug datetime msec  
service timestamps log datetime msec  
service password-encryption  
!  
hostname ausnml-3825-01  
!  
boot-start-marker  
boot system flash c3825-adventerprisek9-mz.124-9.T.bin  
boot-end-marker  
!  
no logging buffered  
enable secret 5 $1$KbIu$5o8qKYAVpWvyv9rYbrJLi/  
!  
aaa new-model  
!  
aaa authentication login default local  
aaa authentication login sdm_vpn_xauth_ml_1 local  
aaa authorization exec default local  
!  
aaa session-id common  
!  
resource policy  
!  
ip cef  
!  
ip domain name cisco.com  
!  
voice-card 0  
no dspfarm  
!  
!--- Self-Signed Certificate Information crypto pki  
trustpoint ausnml-3825-01_Certificate enrollmnet  
selfsigned serial-number none ip-address none  
revocation-check crl rsaкеypair ausnml-3825-  
01_Certificate_RSAKey 1024 ! crypto pki certificate  
chain ausnml-3825-01_Certificate certificate self-signed  
02 30820240 308201A9 A0030201 02020102 300D0609 2A864886  
F70D0101 04050030 29312730 2506092A 864886F7 0D010902  
16186175 736E6D6C 2D333832 352D3031 2E636973 636F2E63  
6F6D301E 170D3036 30373133 32333230 34375A17 0D323030  
31303130 30303030 305A3029 31273025 06092A86 4886F70D  
01090216 18617573 6E6D6C2D 33383235 2D30312E 63697363  
6F2E636F 6D30819F 300D0609 2A864886 F70D0101 01050003  
818D0030 81890281 8100C97D 3D259BB7 3A48F877 2C83222A  
A1E9E42C 5A71452F 9107900B 911C0479 4D31F42A 13E0F63B  
E44753E4 0BEFDA42 FE6ED321 8EE7E811 4DEEC4E4 319C0093  
C1026C0F 38D91236 6D92D931 AC3A84D4 185D220F D45A411B  
09BED541 27F38EF5 1CC01D25 76D559AE D9284A74 8B52856D  
BCBBF677 0F444401 D0AD542C 67BA06AC A9030203 010001A3  
78307630 0F060355 1D130101 FF040530 030101FF 30230603  
551D1104 1C301A82 18617573 6E6D6C2D 33383235 2D30312E  
63697363 6F2E636F 6D301F06 03551D23 04183016 801403E1  
5EAABA47 79F6C70C FBC61B08 90B26C2E 3D4E301D 0603551D  
0E041604 1403E15E AABA4779 F6C70CFB C61B0890 B26C2E3D  
4E300D06 092A8648 86F70D01 01040500 03818100 6938CEA4  
2E56CDDF CF4F2A01 BCD585C7 D6B01665 595C3413 6B7A7B6C  
FOA14383 4DA09C30 FB621F29 8A098FA4 F3A7F046 595F51E6  
7C038112 0934A369 D44C0CF4 718A8972 2DA33C43 46E35DC6  
5DCAE7E0 B0D85987 A0D116A4 600C0C60 71BB1136 486952FC  
55DE6A96 1135C9D6 8C5855ED 4CD3AE55 BDA966D4 BE183920  
88A8A55E quit username admin privilege 15 secret 5  
$1$jm6N$2xNfhupbAinq3BQZMRzrW0 username ausnml privilege
```

```

15 password 7 15071F5A5D292421 username fallback
privilege 15 password 7 08345818501A0A12 username austin
privilege 15 secret 5 $1$3xFv$W0YUsKDxladDc.cVQF2Ei0
username sales_user1 privilege 5 secret 5
$1$2/SX$ep4fsCpodeyKaRji2mJkX/ ! interface
GigabitEthernet0/0 ip address 192.168.0.37 255.255.255.0
duplex auto speed auto media-type rj45 ! interface
GigabitEthernet0/1 ip address 172.22.1.151 255.255.255.0
duplex auto speed auto media-type rj45 ! ip route
0.0.0.0 0.0.0.0 172.22.1.1 ! ip http server ip http
authentication local ip http timeout-policy idle 600
life 86400 requests 100 ! control-plane ! line con 0
stopbits 1 line aux 0 stopbits 1 line vty 0 4 exec-
timeout 40 0 privilege level 15 password 7
071A351A170A1600 transport input telnet ssh line vty 5
15 exec-timeout 40 0 password 7 001107505D580403
transport input telnet ssh ! scheduler allocate 20000
1000 ! !--- WebVPN Gateway webvpn gateway
WidgetSSLVPNGW1 hostname ausnml-3825-01 ip address
192.168.0.37 port 443 http-redirect port 80 ssl
trustpoint ausnml-3825-01_Certificate inservice ! webvpn
context SalesContext ssl authenticate verify all ! !---
Identify resources for the SSL VPN session url-list
"InternalWebServers" heading "WidgetWebServers" url-text
"WidgetWeb" url-value "http://172.22.1.30" url-text
"OWA" url-value "http://172.22.1.50/exchange" ! nbns-
list NBNSservers nbns-server 172.22.1.30 ! !--- Identify
the policy which controls the resources available policy
group policy_1 url-list "InternalWebServers" nbns-list
"NBNSservers" functions file-access functions file-
browse functions file-entry hide-url-bar citrix enabled
default-group-policy policy_1 gateway WidgetSSLVPNGW1
max-users 2 inservice ! end

```

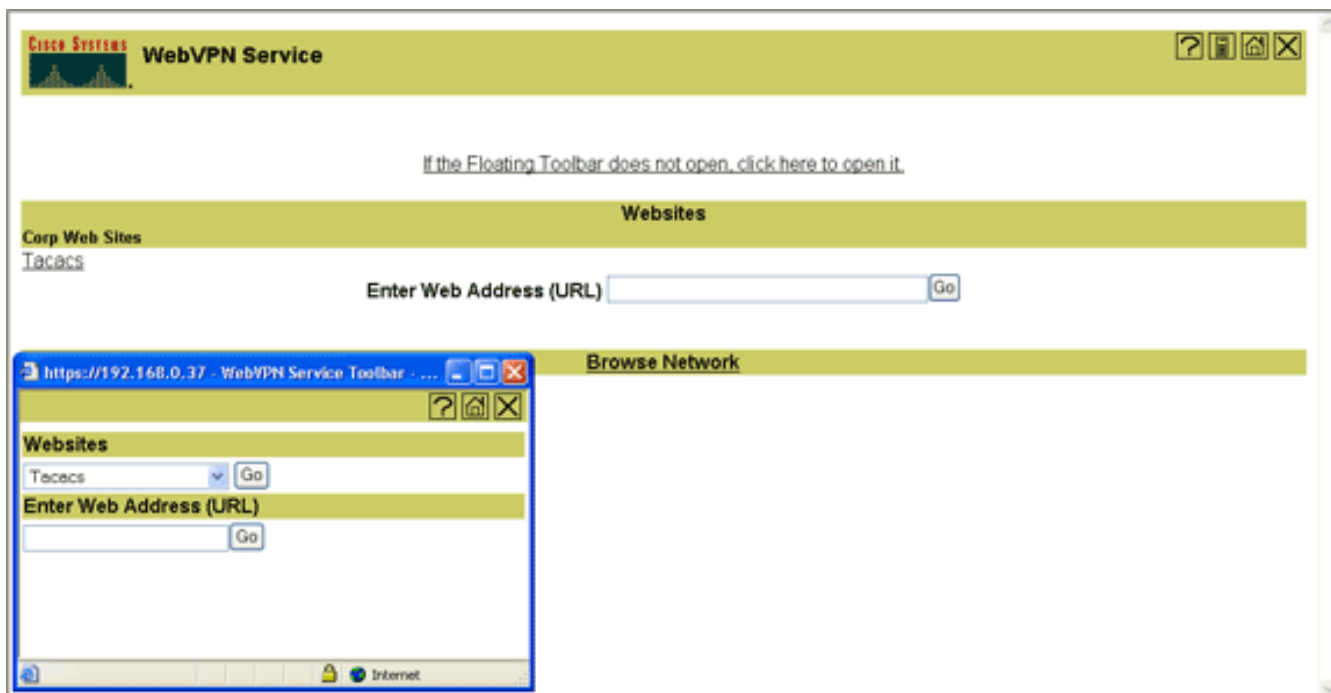
## Vérifiez

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

## Procédure

Exécutez ces procédures afin de confirmer que votre configuration fonctionne correctement :

- Testez votre configuration avec un utilisateur. Entrez **https://WebVPN\_Gateway\_IP\_Address** dans un navigateur Web compatible SSL ; où *WebVPN\_Gateway\_IP\_Address* est l'adresse IP du service WebVPN. Après avoir accepté le certificat et entré un nom d'utilisateur et un mot de passe, un écran semblable à cette image devrait apparaître.



- Vérifiez la session VPN SSL. Dans l'application SDM, cliquez le bouton **Monitor** , puis cliquez sur **VPN status**. Développez **WebVPN (All Contexts)**, développez le contexte approprié, et choisissez **Users**.
- Vérifiez les messages d'erreur. Dans l'application SDM, cliquez le bouton **Monitor**, cliquez sur **Logging**, puis cliquez sur l'onglet **Syslog** .
- Affichez la configuration en cours pour le périphérique. Dans l'application SDM, cliquez le bouton de **Configure**, et puis cliquez sur **Additional Tasks**. Développez **Configuration Management**, et choisissez **Config Editor**.

## Commandes

Plusieurs commandes **show** sont associées au WebVPN. Vous pouvez exécuter ces commandes dans l'interface de ligne de commande (CLI) afin d'afficher les statistiques et autres informations. Pour obtenir des informations détaillées à propos des commandes **show**, reportez-vous à [Vérification de la configuration de WebVPN](#).

**Remarque:** L'[Outil Interpréteur de sortie](#) (clients [enregistrés](#) uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

## Dépannez

Utilisez cette section pour dépanner votre configuration.

**Remarque:** N'interrompez pas la commande **Copy File to Server** et n'accédez pas à une fenêtre différente pendant que la copie est en cours. L'interruption de l'opération peut entraîner l'enregistrement d'un fichier incomplet sur le serveur.

**Remarque:** Les utilisateurs peuvent envoyer et télécharger les nouveaux fichiers à l'aide du client WebVPN, mais l'utilisateur n'est pas autorisé à substituer les fichiers dans le Common Internet File System (CIFS) sur le WebVPN à l'aide de la commande **Copy File to Server**. L'utilisateur reçoit ce message lorsqu'il tente de substituer un fichier sur le serveur :

Unable to add the file

## Procédure

Complétez ces étapes afin de dépanner votre configuration :

1. Assurez-vous que les clients désactivent les bloqueurs de fenêtres publicitaires.
2. Assurez-vous que les clients ont activé les cookies.
3. Assurez-vous que les clients utilisent les navigateurs Web Netscape, Internet Explorer, Firefox ou Mozilla.

## Commandes

Plusieurs commandes **debug** sont associées à WebVPN. Pour obtenir des informations sur ces commandes, reportez-vous à [Utilisation des commandes de débogage de WebVPN](#).

**Remarque:** L'utilisation des commandes **debug** peut avoir un impact négatif sur votre périphérique Cisco. Avant d'utiliser les commandes **debug**, référez-vous à la section **Informations importantes sur les commandes Debug**.

## Informations connexes

- [Cisco IOS SSLVPN](#)
- [Cisco IOS SSLVPN Q&A](#)
- [Exemple de configuration de VPN SSL \(WebVPN\) client léger sur IOS avec SDM](#)
- [Exemple de configuration d'un client VPN SSL \(SVC\) sur IOS avec SDM](#)
- [Support et documentation techniques - Cisco Systems](#)